BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

[Additional counsel listed on signature page]

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

In re InMarket Media Location Data Tracking Litigation

Case No. 3:24-cv-00511-JSC

CONSOLIDATED AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Judge: Hon. Jacqueline Scott Corley

Plaintiffs Autry Willis and Kenneth Kruger ("Plaintiffs"), by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves and their counsel, which are based on personal knowledge, against Defendant InMarket Media, LLC. ("InMarket" or "Defendant").

NATURE OF THE ACTION

1. InMarket violates state law by acquiring and tracking consumers' precise geolocation data and other data without authorization, aggregating it with other data points, and then monetizing the data.

2. It does so through two different channels: (1) InMarket-owned and -operated applications and (2) use of spyware called "InMarket SDK" which is imbedded on numerous third-party applications.

3. The data InMarket collects and uses can include consumers' private movements to and from sensitive locations, like locations associated with medical care, reproductive health, religious worship, mental health, rallies, demonstrations, or protests.

4. In addition to acquiring this private data without consumers' informed consent, InMarket fails to notify consumers that it then aggregates that location data with other data points to develop consumer profiles. Nor does InMarket notify consumers that this data will be used for targeted advertising. It does all of this without consumers' consent.

5. Plaintiffs are individuals who assert claims on behalf of themselves and class members for violations of California privacy statutes and unjust enrichment.

6. By selling this data without consent, Defendant has been unjustly enriched and has violated Plaintiffs' privacy rights, state consumer protection laws, and privacy statutes.

PARTIES

7. Plaintiff Autry Willis is a resident of Oakland, California. Plaintiff Willis downloaded a third-party phone application which contained geolocation data tracking technology ("App"). At the time, Plaintiff Willis believed that the App would not transfer her geolocation data to another entity for the purposes of selling said data. However, that was not the case: the App sent location

data to Defendant when Plaintiff Willis used the App. During that entire time, the App tracked the geolocation of Plaintiff Willis. In turn, Defendant tracked Plaintiff Willis's geolocation in California, and then sold that data for profit. Plaintiff Willis suffered her primary injury in California.

8. During the time Plaintiff Willis used the App, Defendant took Plaintiff Willis's geolocation data from the App and then sold Plaintiff Willis's location data to other third parties.

9. Plaintiff Willis has not consented to have her geolocation data sold to third parties for valuable consideration. If Plaintiff Willis had been aware that Defendant would receive and sell her geolocation data to third parties, Plaintiff Willis would not have used the App.

10. Plaintiff Kenneth Kruger is a resident of Palo Alto, California. Plaintiff Kruger downloaded an App. At the time, Plaintiff Kruger believed that the App would not transfer his geolocation data to another entity for the purposes of selling said data. However, that was not the case: the App sent location data to Defendant when Plaintiff Kruger used the App. During that entire time, the App tracked the geolocation of Plaintiff Kruger. In turn, Defendant tracked Plaintiff Kruger's geolocation in California, and then sold that data for profit. Plaintiff Kruger suffered his primary injury in California.

11. During the time Plaintiff Kruger used the App, Defendant took Plaintiff Kruger's geolocation data from the App and then sold Plaintiff Kruger's location data to other third parties.

12. Plaintiff Kruger has not consented to have his geolocation data sold to third parties for valuable consideration. If Plaintiff Kruger had been aware that Defendant would receive and sell his geolocation data to third parties, Plaintiff Kruger would not have used the App.

13. Defendant InMarket Media, LLC, is a Delaware limited liability corporation with its principal place of business in Austin, Texas.

JURISDICTION AND VENUE

14. Jurisdiction is proper in this Court pursuant to the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2) because this is a class action in which at least one member of the class is a citizen of a state different from any Defendant, the amount in controversy exceeds $5 million, exclusive of interest and costs, and the proposed class contains more than 100 members.

15. This Court has personal jurisdiction over Defendant because a substantial portion of the events giving rise to this cause of action occurred here and Defendant otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in California. Plaintiffs are domiciled and suffered their primary injuries in this District.

16. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a substantial part of the events or omissions giving rise to the claims asserted herein occurred in this District.

FACTUAL ALLEGATIONS

A. InMarket collects sensitive information from App users on over 300 million mobile devices.

17. InMarket is a digital marketing platform and data aggregator.

18. It collects consumer location data through applications InMarket owns and its software development kit (the InMarketSDK) incorporated into third-party mobile applications.

19. InMarket SDK is a collection of development tools that can be incorporated into a mobile application.

20. InMarket SDK's function is to collect the location data of all mobile application users who have InMarket SDK spyware embedded in their Apps, and transmit the consumer's precise location back to Defendant.

21. Thus, through the use of its spyware, InMarket monitors, tracks, and identifies consumers in real time, including Plaintiffs and other putative class members.

22. Defendant fails to notify consumers that their location data will be used for targeted advertising and fails to verify that Apps incorporating the InMarket SDK have notified consumers of such use.

23. Defendant incorporates InMarket SDK into more than 300 third-party Apps, which have been downloaded onto over 390 million unique devices since 2017.

24. Apps that incorporate the InMarket SDK request access to the location data generated by a mobile device's operating system.

25. Critically, the InMarket SDK receives the device's precise latitude and longitude, along with a timestamp and unique mobile device identifier, as often as the mobile device's

operating system provides it— ranging from almost no collection when the device is idle, to every few seconds when the device is actively moving—and transmits it directly to Defendant's servers.

26. As a result, from 2016 to the present, about 100 million unique devices sent Defendant location data *each year*.

27. Defendant collects sensitive information from consumers, including where they live, where they work, where they worship, where their children go to school or obtain child care, where they received medical treatment (potentially revealing the existence of medical conditions), whether they went to rallies, demonstrations, or protests (potentially revealing their political affiliations), and any other information that can be gleaned from tracking a person's day-to-day movements.

28. This information is collected with several identifiers (including a unique mobile device identifier). Defendant has retained this information for up to five years.

29. InMarket uses the consumer data to facilitate targeted advertising to consumers on their mobile devices for the company's clients, which include brands and advertising agencies.

30. Defendant fails to notify consumers that their location data will be used for targeted advertising and fails to verify that apps incorporating the InMarket SDK have notified consumers of such use.

B. Defendant monetizes users' location data through targeted advertising.

31. Defendant sorts consumers based on their visits to points of interest into audience segments to which it can target advertising.

32. Defendant has created or maintains almost two thousand distinct advertising audience segments.

33. For example, an InMarket brand client can target shoppers who are likely to be low-income millennials; well-off suburban moms; parents of preschoolers, high-school students, or kids who are home-schooled; Christian church goers; convenience-sensitive or price-sensitive; single parents or empty-nesters; affluent savers or blue collar workers; "healthy or wealthy" or "wealthy and not healthy," to name only a selection of the categories InMarket offers or has offered to its brand clients.

34. InMarket classifies audiences based on both past behavior and predictions it makes about consumers based on that behavior.

35. For example, if a consumer's past location data shows that she has visited a car dealership, InMarket can combine that information with the consumer's attributes purchased from other sources (age, income, family structure, education level), and can potentially predict that she may be in the market for a certain type of vehicle.

36. The InMarket SDK displays the ads and determines which ads appear in which apps incorporating the SDK.

37. Defendant additionally offers advertisers a product that sends push notifications based on a consumer's location and "geofencing," the creation of a virtual fence around a particular point of interest. When the InMarket SDK transmits a location that is inside a virtual fence, the app will send a push notification for a particular ad.

38. For example, a consumer who is within 200 meters of a pharmacy might see an ad for toothpaste, cold medicine, or some other product sold at that location.

39. Finally, Defendant also makes its advertising audience segments available on real-time bidding platforms. An advertiser using one of these platforms can select an advertising audience and identify the amount that it is willing to pay (that is, its bid) each time its ad appears on a mobile device that is a part of that audience.

40. The advertiser's ad will appear on a particular device if it has the highest bid for that device.

41. Defendant receives revenue each time an advertiser uses one of its audiences in this process.

42. In addition to incorporation of the InMarket SDK into third-party apps, Defendant has incorporated the InMarket SDK into mobile applications that it owns and operates ("InMarket Apps"). InMarket Apps consist of applications InMarket created soon after the company's formation and mobile applications it acquired as part of a campaign to expand its reach and location database. The former applications include CheckPoints, which offers shopping rewards for completing tasks such as watching videos and taking online quizzes, and ListEase, which helps

consumers create shopping lists. These applications have been downloaded onto over 30 million unique devices since 2017.

43. Since 2010, InMarket has offered the CheckPoints app on both the iOS and Android platforms. InMarket's CheckPoints app is marketed as a "rewards app," and promises users "easy money—earn as you shop." It tells consumers to "join the millions earning free gift cards and more every day." Users of the app collect points by performing various tasks (checking into retail locations, watching videos, scanning certain products while in store, taking surveys and quizzes), and then exchange those points for rewards, such as gift cards. The app is free to download and includes in-app advertising.

44. Since 2012, InMarket has offered the ListEase app on both the iOS and Android platforms. The ListEase app markets itself as an electronic shopping list app. The app is free to download and includes in-app advertising.

45. The consent screens used for both the CheckPoints and ListEase apps tell consumers that their location will be used for the app's functionality (earning points and keeping lists), which are misleading half-truths. Thus, users are choosing to share their location with these apps for specific purposes completely unrelated to InMarket's larger advertising-related business.

46. At no point during the consent process for either the CheckPoints or ListEase apps did InMarket also disclose that it was collecting users' precise location, often multiple times per hour, along with data collected from multiple other sources—including through Apps using the InMarket SDK—to build extensive profiles on users to be used to precisely target them with advertising.

47. Although InMarket discloses in its privacy policy that it uses consumer data for targeted advertising, its consent screen does not link to the privacy policy language, and the prompts do not inform consumers of the apps' data collection and use practices.

48. In 2019, InMarket launched a campaign of mobile application acquisitions to expand its consumer reach and location database. To that end, in August 2019, InMarket announced the acquisition of Thinknear, a location-based mobile marketing platform. InMarket's press release on the acquisition described the benefit of the partnership with the following words:

> The acquisition will allow Thinknear's clients to engage at the moment of truth through InMarket's 50 million Comscore-verified smartphone integrations. These direct connections enable brands to identify and engage consumers during multiple touchpoints of the purchase journey, including as they walk into any location in the US. InMarket's Moments technology delivers real-time, premium engagements with customers at precise locations during consideration and decision. InMarket clients will gain access to Thinknear's place-based targeting and Geotype technology, which create valuable high-performing profiles around ideal customers based on location behavior. Thinknear's Geolink is an advanced self-serve dashboard that will give InMarket clients one of their most requested features-- the hands-on ability to launch campaigns themselves from trading desks.[1]

49. In September 2020, InMarket announced the acquisition of assets from NinthDecimal, another location-based attribution and analytics company. The press release noted that "[m]arketers will now have access to an omnichannel platform that includes location and transactional audiences; GeoLink self-service marketing with real-time Moments; Location Conversion Index (LCI) attribution; and a robust set of advanced analytics -- all via one partner."[2]

50. In December 2020, InMarket completed the acquisition of Key Ring, the shopper loyalty app from Vericast.

51. InMarket advertised the acquisition as a further step to "empower brands to reach highly engaged, opted-in shoppers in real-time, while closing the loop on measuring campaign effectiveness," as well as "underscore[] the growing importance of first party data from opted-in consumers, and the value of real-time contextual advertising."[3]

52. In June 2021, InMarket acquired Out of Milk, a shopping list app with millions of downloads. InMarket announced this acquisition as a move to "further bolster its industry-leading suite of owned-and-operated apps, including ListEase, CheckPoints, and Key Ring, that span the journey as shoppers plan, save, and organize. These unique properties are part of InMarket's

[1] *InMarket to Acquire Thinknear, Expand Location-Based Marketing Solutions*, PR NEWSWIRE (Aug. 8, 2019), https://www.prnewswire.com/news-releases/inmarket-to-acquire-thinknear-expand-location-based-marketing-solutions-300899051.html.

[2] *InMarket Acquires Assets from NinthDecimal, Creating the Definitive Leader in Real-Time, Data-Driven Marketing,* PR NEWSWIRE (Sept. 9, 2020), https://www.prnewswire.com/news-releases/inmarket-acquires-assets-from-ninthdecimal-creating-the-definitive-leader-in-real-time-data-driven-marketing-301126032.html.

[3] *InMarket Acquires Key Ring, Expanding its Data-Driven Marketing and Insights* Suite, PR NEWSWIRE (Dec. 10, 2020), https://www.prnewswire.com/news-releases/inmarket-acquires-key-ring-expanding-its-data-driven-marketing-and-insights-suite-301190647.html.

competitive advantage reaching shoppers across all stores and categories. The apps empower brands to reach a variety of highly engaged, opted-in shoppers in real-time."[4] Todd Dipaola, CEO and Founder of InMarket, highlighted the key function of this and the preceding acquisitions: to "scale InMarket" and its breadth of location data.

C. **Defendant fails to verify that users of third-party apps incorporating InMarket's SDK have been notified that their location data will be used to target advertising.**

53. Defendant does little to verify that third-party Apps obtain informed consumer consent before those third-party apps grant InMarket access to consumers' sensitive location data.

54. In fact, InMarket does not require third-party Apps to obtain informed consumer consent at all.

55. InMarket additionally neither collects nor retains records of any disclosures that third-party Apps do provide consumers before accessing their location data.

56. Even if these third-party App developers wanted to provide adequate disclosure to their users about InMarket's use of their location data, InMarket does not provide the developers with sufficient information to provide that notice.

57. Specifically, InMarket's contract with third-party App developers merely states that InMarket will serve ads on the developer's Apps in return for developers passing user information to InMarket, including precise location and advertising identifiers.

58. Defendant does not disclose that information collected from these third-party users will be supplemented and cross-referenced with purchased data and analyzed to draw inferences about those users for marketing purposes.

59. Defendant therefore does not know whether users of hundreds of third-party Apps were informed of their data being collected and used for targeted advertising.

[4] *InMarket Acquires Key Ring, Expanding its Data-Driven Marketing and Insights Suite*, PR NEWSWIRE (June 22, 2021), https://www.prnewswire.com/news-releases/inmarket-acquires-out-of-milk-to-bolster-real-time-contextual-advertising-from-planning-to-purchase-301317186.html.

D. Defendant's practices cause and are likely to cause substantial injury to consumers.

60. Because Defendant combined consumers' location data with other personal information in its databases and systems without confirming user consent, Defendant obtained and used that data without informed user consent, resulting in consumer injury.

61. In addition, after collecting sensitive, precise location data about consumers' daily movements, Defendant retains that information longer than reasonably necessary to accomplish the purpose for which that information was collected and thereby exposes consumers to significant unnecessary risk. Specifically, InMarket has retained consumer location data for five years prior to deletion.

62. This unreasonably long retention period significantly increases the risk that this sensitive data could be disclosed, misused, and linked back to the consumer, thereby exposing sensitive information about that consumer's life.

63. Defendant's comprehensive collection and long-term retention of location data subjects consumers to a likelihood of substantial injury through the exposure of their re-identified location.

FTC'S JANUARY 2023 COMPLAINT AGAINST DEFENDANT

64. In January 2023, the FTC took action against Defendant for allegations that are substantially identical to this complaint.

65. According to the FTC's complaint, Defendant's acts as described above constitutes a violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair or deceptive acts or practices in or affecting commerce."

66. Acts or practices are unfair under Section 5 of the FTC Act if they cause or are likely to cause substantial injury to consumers that consumers cannot reasonably avoid themselves and that is not outweighed by countervailing benefits to consumers or competition. 15 U.S.C. § 45(n).

CLASS ALLEGATIONS

67. ***Class Definition.*** Plaintiffs bring this action on behalf of a class of similarly situated individuals, defined as:

> All persons who reside in California whose data, including but not limited to their geolocation data, was collected by Defendant without their consent.

(the "Class").

68. Excluded from the Class are Defendant and any entities in which Defendant has a controlling interest, Defendant's agents and employees, the judge to whom this action is assigned, and members of the judge's staff, and the judge's immediate family.

69. Subject to additional information obtained through discovery, the foregoing class definition may be modified or narrowed by an amended complaint, or at class certification, including through the use of multi-state subclasses to account for material differences in state law, if any.

70. ***Numerosity.*** Members of the Class ("Class Members") are so numerous that their individual joinder herein is impracticable. On information and belief, members of the Class number in the millions. The precise number of Class Members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Class Members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant and third-party retailers and vendors.

71. ***Commonality and Predominance.*** Common questions of law and fact exist as to all Class Members and predominate over questions affecting only individual Class Members. Common legal and factual questions include but are not limited to:

(a) Whether Defendant's sale of geolocation data without consent constitutes unjust enrichment;

(b) Whether Defendant engaged in the wrongful conduct alleged herein;

(c) Whether Defendant's collection, storage, distribution, and/or use of Plaintiffs' and Class Members' Personal Information violated privacy rights and invaded Plaintiffs' and Class Members' privacy; and

(d) Whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

72. ***Typicality.*** The claims of the named Plaintiffs are typical of the claims of the Class in that the named Plaintiffs' data was sold by Defendant without their consent, and the named Plaintiffs suffered injury as a result of Defendant's conduct.

73. ***Adequacy.*** Plaintiffs are adequate representatives of the Class because their interests do not conflict with the interests of the Class Members they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

74. ***Superiority.*** The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Class Members. Each individual Class Member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

COUNT I
Invasion of Privacy

75. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

76. The California Constitution recognizes the right to privacy inherent in all residents of the State and creates a private right of action against private entities that invade that right.

77. Article I, Section 1 of the California Constitution provides: "All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and

liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."

78. The right to privacy was added to the California Constitution in 1972, through Proposition 11 (called the "Right to Privacy Initiative"). Proposition 11 was designed to codify the right to privacy, protecting individuals from invasions of privacy from both the government and private entities alike: "The right of privacy is the right to be left alone. It is a fundamental and compelling interest . . . . It prevents government and business interests from collecting and stockpiling unnecessary information about us and from misusing information gathered for one purpose in order to serve other purposes or to embarrass us. Fundamental to our privacy is the ability to control circulation of personal information." Ballot Pamp., Proposed Stats. And Amends. To Cal. Const. with arguments to voters, Gen. Elec. (Nov. 7, 1972), argument in favor of Prop. 11, p. 27; *see also Hill v. Colorado*, 530 U.S. 703, 716 (2000) (the right to privacy includes right to be free in one's home from unwanted communication); *Hill v. National Collegiate Athletic Assn.* (1994), 7 Cal.4th 1, 81, (Mosk, J., dissenting).

79. Plaintiffs and the Class Members have a legally protected privacy interest, as recognized by the California Constitution, CIPA, common law, and the 4th Amendment to the United States Constitution.

80. Plaintiffs and Class Members had a reasonable expectation of privacy under the circumstances, as they could not have reasonably expected that Defendant would violate state privacy laws. Plaintiffs and Class Members were not aware and could not have reasonably expected that unknown third party would install software on their mobile devices that would track and transmit their physical location and communications, and share Plaintiffs' and Class Members' sensitive information with other parties.

81. Defendant's conduct violates, at a minimum:

(a) The right to privacy in data, communications and personal information contained on personal devices;

(b) The California Constitution, Article I, Section 1;

(c) The California Wiretapping Act;

(d) The California Invasion of Privacy Act; and

(e) The California Computer Data Access and Fraud Act.

82. Defendant’s conduct in secretly intercepting and collecting Plaintiffs’ and Class Members’ personal information, location data, and communications is an egregious breach of social norms and is highly offensive to a reasonable person.

83. Defendant’s conduct in analyzing, using, and sharing with third parties the personal information and communications that Defendant intercepted and took from Plaintiffs’ and Class Members is an egregious breach of societal norms and is highly offensive to a reasonable person, and violates Plaintiffs’ and Class Members’ reasonable expectations of privacy.

84. Plaintiffs and Class Members did not consent for Defendant to track, collect, or use their personal information and communications.

85. As a direct and proximate result of Defendant's invasion of their privacy, Plaintiffs and Class Members were injured and suffered damages. Plaintiffs and Class Members are entitled to equitable relief and just compensation in an amount to be determined at trial.

86. Defendant was unjustly enriched as a result of its invasion of Plaintiffs’ and Class Members’ privacy.

COUNT II
Violation of the California Computer Data Access and Fraud Act
Cal. Penal Code. § 502

87. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

88. The California legislature enacted the CDAFA with the intent of “expand[ing] the degree of protection afforded to individuals … from tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems.” Cal. Penal Code §502(a). The enactment of CDAFA was motivated by the finding that “the proliferation of computer technology has resulted in a concomitant proliferation of … unauthorized access to computers, computer systems, and computer data.” *Id.*

89. Plaintiffs’ and Class Members’ smartphones constitute “computers” within the scope of the CDAFA.

90. Defendant violated the following sections of the CDAFA:

(a) Section 502(c)(1), which makes it unlawful to "knowingly access[] and without permission . . . use[] any data, computer, computer system, or computer network in order to either (A) devise or execute any scheme or artifice to defraud, deceive, or extort, or (B) wrongfully control or obtain money, property, or data;"

(b) Section 502(c)(2), which makes it unlawful to "knowingly accesses and without permission takes, copies, or makes use of any data from a computer, computer system, or computer network, or takes or copies any supporting documentation, whether existing or residing internal or external to a computer, computer system, or computer network;"

(c) Section 502(c)(7), which makes it unlawful to "knowingly and without permission accesses or causes to be accessed any computer, computer system, or computer network."

91. Defendant knowingly accessed Plaintiffs' and Class Members' smartphones without their permission by including within the SDK that Defendant provides to developers, software that intercepts and transmits data, communications, and personal information concerning Plaintiffs and Class Members.

92. Defendant used data, communications, and personal information that it intercepted and took from Plaintiffs' and Class Members' smartphones to wrongfully and unjustly enrich itself at the expense of Plaintiffs and Class Members.

93. Defendant took, copied, intercepted, and made use of data, communications, and personal information from Plaintiffs' and Class Members' smartphones.

94. Defendant knowingly and without Plaintiffs' and Class Members' permission accessed or caused to be their smartphones by installing—without Plaintiffs' and Class Members' informed consent—software that intercepts and/or takes data, communications, and personal information concerning Plaintiffs and Class Members.

95. Plaintiffs and Class Members are residents of California and used their smartphones in California. Defendant accessed or caused to be accessed Plaintiffs' and Class Members' data,

communications, and personal information from California. On information and belief, Defendant uses servers located in California that allow Defendant to access and process the data, communications and personal information concerning Plaintiffs and Class Members.

96. Defendant was unjustly enriched by intercepting, acquiring, taking, or using Plaintiffs' and Class Members' data, communications, and personal information without their permission, and using it for Defendant's own financial benefit. Defendant has been unjustly enriched in an amount to be determined at trial.

97. As a direct and proximate result of Defendant's violations of the CDAFA, Plaintiffs and Class Members suffered damages.

98. Pursuant to CDAFA Section 502(e)(1), Plaintiffs and Class Members seek compensatory, injunctive and equitable relief in an amount to be determined at trial.

99. Pursuant to CDAFA Section 502(e)(2), Plaintiffs and Class Members seek an award of reasonable attorney's fees and costs.

100. Pursuant to CDAFA Section 502(e)(4), Plaintiffs and Class Members seek punitive or exemplary damages for Defendant's willful violations of the CDAFA.

COUNT III
Use of a Pen Register or Trap and Trace Device
Cal. Penal Code § 638.51

101. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

102. California Penal Code Section 638.50(b) defines a "pen register" as "a device or process that records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, but not the contents of a communication."

103. California Penal Code Section 638.51 prohibits any person from using a pen register without a court order.

104. Defendant's SDK constitutes a "pen register" because it is a device or process that records addressing or signaling information—Plaintiffs and Class Members' location data and personal information—from the electronic communications transmitted by their smartphones.

105. Defendant was not authorized by any court order to use a pen register to track Plaintiffs and Class Members' location data and personal information.

106. As a direct and proximate result of Defendant's conduct, Plaintiffs and Class Members suffered losses and were damaged in an amount to be determined at trial.

COUNT IV
Violation of the California Wiretapping Act
Cal. Penal Code § 631

107. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

108. At all relevant times, there was in full force and effect the California Wiretapping Act, Cal. Penal Code § 631.

109. The California legislature enacted the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, *et seq.*, including the Wiretapping Act, "to protect the right of privacy" of residents of California. Cal. Penal Code § 630.

110. The California legislature was motivated to enact CIPA by a concern that the "advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society." *Id.*

111. The California Wiretapping Act prohibits:

> any person [from using] any machine, instrument, [] contrivance, or in any other manner … [from making] any unauthorized connection, whether physically, electronically, acoustically, inductively, or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system, or who willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section[.]

112. Plaintiffs and Class Members' specific user input events and choices on their mobile devices that are tracked by Defendant's SDK communicates the user's affirmative actions, such as clicking a link, installing an app, selecting an option, or relaying a response, and constitute communications within the scope of the Wiretapping Act.

113. Plaintiffs and Class Members are residents of California, and used their smartphones within California. Accordingly, Defendant intercepts, reads, or attempts to read Plaintiffs' and Class members' data, communications, and personal information in California.

114. On information and belief, Defendant uses servers in California to intercept, track, process, or otherwise use Plaintiffs' and Class Members' data, communications, and personal information within California.

115. Defendant intercepts Plaintiffs' and Class Members' communications while they are in transit to and from Plaintiffs' and Class Members' smartphones and the apps, app developers, and cellphone towers; Defendant transmits a copy of Plaintiffs' and Class Members' communications to itself. Defendant uses the contents of the communications to sell to third parties and in other methods for its own pecuniary gain.

116. Neither Defendant nor any other person informed Plaintiffs and Class members that Defendant was intercepting and transmitting Plaintiffs' private communications. Plaintiffs and Class Members did not know Defendant was intercepting and recording their communications, as such they could not and did not consent for their communications to be intercepted by Defendant and thereafter transmitted to others.

117. Defendant's SDK constitutes a machine, instrument, contrivance, or other manner to track and intercept Plaintiffs' and Class members' communications while they are using their smartphones.

118. Defendant uses and attempts to use or communicate the meaning of Plaintiffs' and Class Members' communications by ascertaining their personal information, including their geolocation and places that they have visited, in order to sell Plaintiffs' and Class Members' personal information to third parties.

119. At all relevant times to this complaint, Defendant intercepted and recorded components of Plaintiffs' and the putative Class' private telephone communications and transmissions when Plaintiffs and other Class Members accessed Defendant's software via their cellular mobile access devices within the State of California.

120. At all relevant times to this complaint, Plaintiffs and other Class Members did not know Defendant was engaging in such interception and recording and therefore could not provide consent to have any part of their private and confidential video conferencing communications intercepted and recorded by Defendant and thereafter transmitted to others.

121. At the inception of Defendant's illegally intercepted and stored geolocation and other personal data, Defendant never advised Plaintiffs or the other Class Members that any part of this sensitive personal data would be intercepted, recorded and transmitted to third parties.

122. Section 631(a) is not limited to phone lines, but also applies to "new technologies" such as computers, the Internet, and email.

123. Defendant's use of its SDK is both a "machine, instrument, contrivance, or … other manner" used to engage in the prohibited conduct at issue here.

124. At all relevant times, by using Defendant's SDK as well as tracking Plaintiffs' and Class Members' geolocation, Defendant intentionally tapped, electrically or otherwise, the lines of internet communication between Plaintiffs and Class Members on the one hand, and the specific sites and locations Plaintiffs and Class Members visited on the other.

125. At all relevant times, by using Defendant's geolocation tracking software technology, Defendant willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and putative Class Members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

126. Plaintiffs and Class Members did not consent to any of Defendant's actions in implementing these wiretaps within its geolocation tracking software. Nor have Plaintiffs or Class

Members consented to Defendant's intentional access, interception, reading, learning, recording, and collection of Plaintiffs and Class Members' electronic communications.

127. Plaintiffs' and the Class Members' devices of which Defendant accessed through its unauthorized actions included their computers, smart phones, and tablets and/or other electronic computing devices.

128. Defendant violated Cal. Penal Code § 631 by knowingly accessing and without permission accessing Plaintiffs and Class Members' devices in order to obtain their personal information, including their device and location data and personal communications with others, and in order for Defendant to share that data with third parties, in violation of Plaintiffs' and Class Members' reasonable expectations of privacy in their devices and data.

129. Defendant violated Cal. Penal Code § 631 by knowingly and without permission intercepting, wiretapping, accessing, taking and using Plaintiffs' and the Class Members' personally identifiable information and personal communications with others.

130. As a direct and proximate result of Defendant's violation of the Wiretapping Act, Plaintiffs and Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

131. Defendant was unjustly enriched by its violation of the Wiretapping Act.

132. Pursuant to California Penal Code Section 637.2, Plaintiffs and Class Members have been injured by Defendant's violation of the Wiretapping Act, and seek damages for the greater of $5,000 or three times the amount of actual damages, and injunctive relief.

COUNT V
Unfair Practices
In Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200

133. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

134. At all relevant times there was in full force and effect the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code § 17200, *et seq.*, which prohibits, *inter alia*, "any unlawful, *unfair*, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code § 17200 (emphasis added).

135. Defendant engaged in business acts and practices which are "unfair" under the UCL, including surreptitiously collecting, tracking, using and disseminating Plaintiffs' and Class Members' personal information, geolocation data, and communications.

136. Defendant also engaged in a number of practices designed to perpetuate the scheme and the stream of revenue it generates. Those practices, which are unfair separately and particularly when taken together, include but are not limited to invasion of Plaintiffs' and Class members' privacy; surreptitiously tracking Plaintiffs' and Class members' location; surreptitiously accessing Plaintiffs' and Class Members' cellphones without authorization; surreptitiously obtaining personal data from Plaintiffs' and Class members' cellphones; surreptitiously intercepting and recording Plaintiffs' and Class Members' communications.

137. Defendant also engaged in a number of practices designed to perpetuate the scheme and the stream of revenue it generates. Those practices, which are unfair separately and particularly when taken together, include but are not limited to invasion of Plaintiffs' and Class Members' privacy; surreptitiously tracking Plaintiffs' and Class Members' location; surreptitiously accessing Plaintiffs' and Class Members' cellphones without authorization; surreptitiously obtaining personal data from Plaintiffs' and Class Members' cellphones; surreptitiously intercepting and recording Plaintiffs' and Class Members' communications.

138. Unfair acts under the UCL have been interpreted using three different tests: (1) whether the public policy which is a predicate to a consumer unfair competition action under the unfair prong of the UCL is tethered to specific constitutional, statutory, or regulatory provisions; (2) whether the gravity of the harm to the consumer caused by the challenged business practice outweighs the utility of the defendant's conduct; and (3) whether the consumer injury is substantial, not outweighed by any countervailing benefits to consumers or competition, and is an injury that consumers themselves could not reasonably have avoided. Defendant's conduct alleged is unfair under all of these tests.

139. As a direct and proximate result of Defendant's unfair practices, Plaintiffs and Class Members were injured and suffered damages, a loss of privacy, and loss of the value of their personal information in an amount to be determined at trial.

140. Plaintiffs seeks to enjoin further unfair acts or practices by Defendant, to obtain restitution and disgorgement of all monies generated as a result of such practices, and for all other relief allowed under California Business & Profession Code §17200.

COUNT VI
Unlawful Practices
In Violation of the California Unfair Competition Law
Cal. Bus. & Prof. Code § 17200

141. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

142. At all relevant times there was in full force and effect the California Unfair Competition Law ("UCL"), Cal. Bus. & Prof. Code §17200, *et seq.*, which prohibits, *inter alia*, "any *unlawful*, unfair, or fraudulent business act or practice" and "unfair, deceptive, untrue, or misleading advertising." Cal. Bus. & Prof. Code §17200 (emphasis added).

143. In the course of their business, Defendant repeatedly and regularly engaged in unlawful acts or practices that imposed a serious harm on consumers, including Plaintiffs and Class Members.

144. Defendant's acts and practices are unlawful because Defendant violated, and continues to violate:

(a) The Constitution of California, Article I, Section 1;

(b) The California Computer Data Access and Fraud Act;

(c) The California Invasion of Privacy Act; and

(d) Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45.

145. As a direct and proximate result of Defendant's unlawful practices, Plaintiffs and Class Members were injured and suffered damages, a loss of privacy, and loss of value of their personal information in an amount to be determined at trial.

146. Plaintiffs seek to enjoin further unlawful acts or practices by Defendant, to obtain restitution and disgorgement of all monies generated as a result of such practices, and for all other relief allowed under California Business & Professions Code §17200.

COUNT VII
Unjust Enrichment or Restitution

147. Plaintiffs reallege and reincorporate by reference all paragraphs alleged above.

148. Plaintiffs and members of the Class conferred a benefit on Defendant through the use and dissemination of Plaintiffs' and Class Members' personal information, geolocation data, and communications.

149. Defendant received and is in possession of Plaintiffs' and Class Members' personal information, geolocation data, and communications, which Defendant used and disseminated for its own monetary benefit.

150. It is unjust under the circumstances for Defendant to retain the benefit conferred by Plaintiffs and Class members without compensating them.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of all others similarly situated, seek judgment against Defendant, as follows:

(a) For an order certifying the Class under Fed. R. Civ. P. 23 and naming Plaintiffs as representatives of the Class and Plaintiffs' attorneys as Class Counsel;

(b) For an order declaring the Defendant's conduct violates the statutes referenced herein;

(c) For an order finding in favor of Plaintiffs, and the Class on all counts asserted herein;

(d) For compensatory, statutory, and punitive damages in amounts to be determined by the Court and/or jury;

(e) For prejudgment interest on all amounts awarded;

(f) For an order of restitution and all other forms of equitable monetary relief;

(g) For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit.

JURY TRIAL DEMANDED

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Dated: July 2, 2024

BURSOR & FISHER, P.A.

By: /s/ *L. Timothy Fisher*
L. Timothy Fisher

L Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
E-mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Joseph I. Marchese (*pro hac vice* forthcoming)
Julian C. Diamond (*pro hac vice* forthcoming)
1330 Avenue of the Americas, 32nd Floor
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-Mail: jmarchese@bursor.com
jdiamond@bursor.com

AHDOOT & WOLFSON, PC
Tina Wolfson (SBN 174806)
Robert Ahdoot (SBN 172098)
Theodore Maya (SBN 223242)
Deborah De Villa (SBN 312564)
Sarper Unal (SBN 341739)
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Tel: 310.474.9111
Fax: 310.474.8585
Email: twolfson@ahdootwolfson.com
rahdoot@ahdootwolfson.com
tmaya@ahdootwolfson.com
ddevilla@ahdootwolfson.com
sunal@ahdootwolfson.com

AHDOOT & WOLFSON, PC
Melissa Clark (*pro hac vice*)
521 5th Avenue, 17th Floor
New York, NY 10175
Tel: 310.474.9111

Fax: 310.474.8585
Email: mclark@ahdootwolfson.com

Attorneys for Plaintiffs